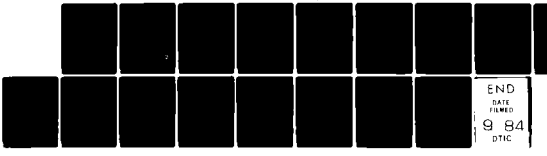
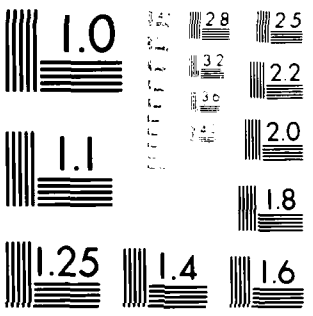
AD-A145 193 INFORMATION SYSTEMS SECURITY AND PRIVACY(U) RAND CORP 1/1
SANTA MONICA CA W H WARE NOV 83 RAND/P-6930

UNCLASSIFIED F/G 9/2 NL



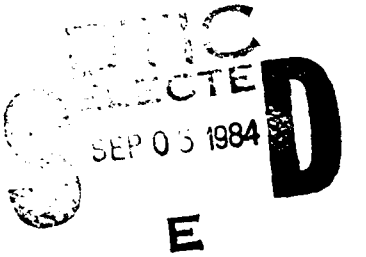

1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6

(2)

INFORMATION SYSTEMS, SECURITY, AND PRIVACY

Willis H. Ware

November 1983



P-6930

The Rand Corporation
Santa Monica, California 90406

Testimony of

Willis H. Ware

INFORMATION SYSTEMS, SECURITY, AND PRIVACY

Before the Subcommittee on Transportation, Aviation and Materials, Committee on Science and Technology, United States House of Representatives[1]

October 24, 1983

INTRODUCTION

My name is Willis H. Ware. I am a member of the Corporate Research Staff of The Rand Corporation, but the views I state today are solely my own; they in no way reflect a position of The Rand Corporation nor of its research clients. Furthermore, my views do not come from a specific contract, but rather reflect a decade of my attention to the issue. I am an electrical engineer by training, but have specialized in the field of computer technology for over thirty years.

My credentials for addressing the issue include the following. In 1967, I was the first to bring the issue of computer security to the attention of the technical field by organizing a special session on the subject at a Joint Computer Conference in the spring of that year. Subsequently, I chaired a Defense Science Board (Department of Defense) committee to look at the issue of computer security which had never been examined comprehensively anywhere in government. The report was a definitive treatment of the subject, and to this day remains an excellent primer. I have furnished three copies of that document to this committee as background information.

---

[1]Additional material on electronic mail was orally presented but did not appear in the originally submitted testimony. This version includes the additional material and has been slightly edited and annotated.

Because of my work in computer security, I was asked in the early 1970s to join a special advisory group to the Secretary of HEW, and I subsequently became its chairman. Its report, *Records, Computers and the Rights of Citizens,* was the first comprehensive treatment of the matter at the federal level. It provided the intellectual foundation for the Federal Privacy Act of 1974, which among other things created the Privacy Protection Study Commission of which I was a member and vice chairman.

In addition to my participation in the activities noted above, I have also spoken and written widely on the subject. In particular, I presented a paper, *Policy Aspects of Privacy and Access,* to a National Science Foundation symposium. Although the paper will be published by Crane-Russak as a special double issue of its journal *The Information Society,*[2] I will forward three copies of it to the committee for background information.

STATEMENT

Congressman Glickman, it is a pleasure to have been invited here today to talk with you about a subject that is of such importance, not only to me professionally but also to the country. Since time is limited this morning, my presentation will be in the nature of a hopscotch over a variety of points and ideas that I think will be of significance for you. I will elaborate or expand in any detail at your request or on another occasion.

Let me first clarify the relationship between security and privacy, where I use the latter term in the context of record-keeping privacy; namely, the use of information about people to make decisions and judgments about them. Record-keeping privacy concerns personal information kept in computer-based systems, and the essence of it is protecting such information and controlling its use for authorized purposes. In contrast, computer security is that body of technology, techniques, procedures, and practices that provides the protective mechanisms to assure the safety of both the computer systems themselves

[2]Issue 3/4, Vol. 2 is in press. Anticipated date of publication December 1983.

and the information within them; and, in addition, limits access to such information solely to authorized users. Computer security is of importance whether the information to be protected is personal in nature and therefore relative to privacy; whether it is defense in nature and therefore related to the security of the country; or whether it is sensitive in nature and therefore relevant to corporate welfare in the private sector. The important point to be noted is that a comprehensive set of security safeguards within and around a computer-based information system is an essential prerequisite for assuring personal privacy. To operate such a system without relevant safeguards is a sham against privacy assurance.

The computer security issue must be seen as analogous to the classical offense/defense situation. As computer security safeguards become stronger, the offenses against them will become more sophisticated and the cycle will repeat. Therefore, no organization or Congress can assume that the computer security issue is one that can be looked at and forgotten. It first surfaced on the professional scene only fifteen years ago; we are still low on the learning curve with regard to knowing how to incorporate comprehensive protection mechanisms in our systems. It is an evolving issue, not a static end-of-the-road one to be dismissed. Therefore, I would recommend to you that:

> It be a standing agenda item for this or other committees of the Congress to look at every year or so for at least the next five and possibly the next ten years.

Next, let me contrast the security situation in the defense environment versus that in the commercial/industrial world. Within defense the threat against computer-based systems includes the full technical resources of advanced major world powers, where such threats can be mounted with substantial funding and other resources. In the Department of Defense context, therefore, the threat includes intense technical aspects as well as aspects involving people -- such as buying them for subversive actions. On the other hand, the defense community does go through an investigative process to grant formal clearances to people; therefore, it has substantial assurance of trustworthiness.

In the commercial sector, on the other hand, the technical threat is at present minimal. The big threat is people within the systems themselves. If one examines, for example, the Parker/SRI database of computer-related criminal actions, he finds that the great bulk of them have been perpetrated by an individual who was authorized to interact with the system and who knew enough about it to exploit it for personal gain. Furthermore, there is generally little attention paid in the commercial world to establishing trustworthiness of individuals in critical and sensitive positions within a computer-based information system. Some corporations do essentially nothing by way of assuring the trustworthiness of critical individuals; others take the minimal step of requiring that individuals be bondable -- a really minimum level of assurance of trustworthiness; and very few, perhaps none, engage in a comprehensive background investigation. When the private sector gets the "people problem" dimension of the threat against its computer systems under control, and the simple technical threats protected against, then sophisticated technical threats will become more important.

Let us examine the last point more closely. What can we do about the simple technical threats, such as those used in the Milwaukee-414 caper, or those involved in the various criminal acts of the SRI database? The dominant point is: technology is not the issue. There are ample technological safeguards that can be installed, and would be effective against many of the crimes that have been perpetrated and against many of the mischievous pranks that have occurred. There are also procedural and administrative safeguards that can be important deterrents. In the private sector, we need only the corporate will to address the problem, and the corporate commitment to put the issue on the same level of concern as that of protecting other valuable resources. By implication, we also need the corporate commitment to spend the modest sums needed. Importantly, we need private sector users of computers to signal the computer industry that technical safeguards are wanted, are essential, and will be paid for.

Do not underestimate that last point. Until the IBMs, the DECs, the Burroughs, the UNIVACs, and others of the commercial computer industry understand that their respective customer bases want technical security safeguard features, the product lines will not have them. I would suggest that the government has a major leverage on this issue. It can make mandatory the inclusion of appropriate technical security features in computer systems that it procures.

Consider now the people aspect of the threat. It is a hard one to counter because one cannot legislate trustworthiness, and even the most extensive background investigation may not reveal deeply hidden or latent problems. To start with, we must do all that is possible with technical procedural safeguards; a good array of them will fend off many people problems. We might take legal steps. One possibility for encouraging private sector response would be to create a basis in law for acting against the record-keeping installation for contributory negligence should state-of-the-art security safeguards not be in place.

It might be possible to extend the principle of the attractive nuisance, which in a sense is really what happens with 414-type activities. A computer system is not a physically attractive nuisance, but rather an intellectually attractive one that causes imaginative or criminally minded people to hack at computer systems. The legal principle of an attractive nuisance encourages people to build fences around swimming pools; perhaps the same notion can be elaborated or reinterpreted to encourage operators of computer systems to install appropriate safeguards.

Incidentally, for the most part we are not talking about large dollar investments. Clearly, if an organization operates its computer center behind a plateglass window and encourages casual visitors to wander among the equipment, there might be a significant initial investment to physically secure the facility and provide it with appropriate physical and fire protection. Beyond this phase though, many organizations find that important security safeguards can be installed as part of changes that are made for other reasons and the costs of such security changes are frequently unnoticeable. Cost will not be zero but neither will it be burdensome.

What about technical safeguards against the people threat? There are attractive options and I will illustrate with two examples. When an individual logs on to a computer system, he is normally requested to supply personal identification and a password which, in effect, is an authentication of his identity. Someone attempting to penetrate a computer system tries to guess his way in by masquerading as a legitimate user. Most systems today permit an indefinite number of log-on trials. It therefore is feasible for a perpetrator to program a small computer to systematically try words, combinations of letters and characters, or other possible passwords until one is found that works. The movie *WarGames* showed such a penetration very realistically and accurately.

Clearly, this is an undesirable and unsafe arrangement. There is no reason why a computer should not disconnect an individual after some number of attempts, such as three or five, and keep him disconnected until his authenticity has been assured. Three weeks ago you heard from Mr. McClary of the Los Alamos National Laboratory. He did not mention the arrangement at Los Alamos with regard to passwords, but since I happened to have discussed computer security with LANL recently, let me indicate how it is handled.

If an individual -- and it might be a respected, established senior researcher of national repute -- fails to log on after a number of tries, such as three or five, his account is completely disabled until he personally appears at the security office and explains why he was unable to type his password successfully after the prescribed number of tries. If he fails to log on successfully in a second series of attempts, his supervisor is required to explain in writing why the individual in question seems not able to type correctly. While this process might seem stringent and it is undoubtedly annoying to an individual, nonetheless disabling repeated log-on attempts is an appropriate arrangement to fend off penetration attempts by guessing in. The media reported the Security Pacific National Bank as having diverted a presumed penetrator by offering him a game to play while tracing the origin of the call; such an approach is obviously a very imaginative and appropriate deterrent.

A second example. Since every computer system has to be started at some time, invariably there is a mechanism for accomplishing what is called the initial software load. Often this takes the form of a button, a switch, or a sequence of actions by the console operator. Imagine a scenario in which an operator on the graveyard shift finds the machine inactive and decides to do something in his own behalf such as illegally copying a sensitive file of information. Having done so, he simply reloads the machine as though it had stopped for some reason; there will be no record of what he has surreptitiously done. There are obvious technical offsets to such malfeasance by operators, but they do not exist in marketed machines. Even the procedure of two-person control as used by the military would be a deterrent.

We need a menu of technical features that machines should have in order to help offset aspects of the people-threat problem. Let me offer you a recommendation:

> Task the Institute of Computer Science and Technology of the National Bureau of Standards to produce such a list of options, and consider making it mandatory in government acquisitions of computer systems.

Now to the question of where the wisdom will come from within government to deal with the broad dimensions of computer security. I remind you that there are technical aspects of it related to not only hardware and software but also to communication security and radiation security (TEMPEST); but in addition there are physical, procedural, personnel, and administrative aspects. Every one has to be attended to, especially the last three. A computer system with the best technical safeguards can be readily penetrable if it is operated with sloppy and careless procedural and administrative arrangements by people with uncertain backgrounds. Where will the government develop the guidance that it needs on these many dimensions?

Many of them are already in hand because they are understood for other reasons. For example, the Department of Defense certainly knows how to deal with physical security and with personnel security; its

experience is available to other agencies of government as might be needed. The TEMPEST radiation issue is understood and safeguards for it exist. There are many private organizations today that can advise on fire protection, physical protection, personnel control, and the likes. But, in government where does the technical software/hardware guidance come from? And where does the contextual administrative and management guidance come from?

What are the government's principal assets? You heard from them on October 17; the Institute of Computer Science and Technology of the National Bureau of Standards, the Computer Security Center of the National Security Agency, and GSA. Take the CSC first.

The focus of concern in CSC is "trusted systems" and especially "trusted software." Understand the word "trust" as you would intuitively think of it; namely, one can have confidence that the system or the software will do what it is supposed to do, and one can have confidence that it will not do what it is not supposed to do. Keep in mind that CSC is a Department of Defense entity, and therefore its focus of concern is on defense systems and especially with a sophisticated technical threat. It can and it will provide expertise to address the software/hardware issue.

I suggest to you that the problem of incorporating security safeguards in software -- and of knowing that they are really there and functioning correctly -- is so difficult technically and the country's expertise is so miniminal on it, that we can staff only one such Center at the moment. We would be wise to place all our eggs in this one basket with regard to trusted software until additional expertise can be developed over the next five to ten years. While CSC will also be concerned with other security aspects of systems that contain both computers and communications, it will not be concerned with the general administrative and procedural environment in which secure systems must be operated.

The ICST of the NBS is also involved in technical work. For example, it was the source of the Digital Encryption Standard some five years ago and it made a very significant contribution to the protection of information while in transit through a communication network. It also publishes the *Federal Information Processing Standards* which deal

with such issues as the use of DES, the management of keys for it, risk assessment and risk management. But, neither the ICST nor the CSC is providing the comprehensive overview that can stipulate:

- Here is how one runs a computer system and does it securely.
- Here are the procedural and administrative safeguards that must be in place.
- Here are the specific risks that people represent.
- Here are the countermeasures that can be taken against the nontechnical threats.
- Here are the management mechanisms to oversee security safeguards.
- Here are the general protective precautions that can be taken. Etc.

No entity in government has addressed the general policy issue of what constitutes a comprehensive top-to-bottom prescription for installing security controls, nor identified the many dimensions of such a policy and made it available as guidance. It is being done piecemeal; every agency is inventing it for itself or not doing it. There is some policy guidance in the DoD in the form of general regulations and directives. There are interagency committees and technical organizations in which people can trade ideas and talk with one another. In the private sector, major corporations have built their own policy structures and implementing details.

The government truly needs a comprehensive "how to do it" document that sets forth preferred practices and procedures for operating a secure computer system. The private sector could well use the same thing. The ideas and the information exist but everything is scattered. The information is not collected and coordinated; it is in people's heads or embodied in daily activities and not otherwise documented. We -- the country -- need to organize the collective wisdom of what is known and what is being done and make it widely available.

As a first step, I would note that the General Services Administration has had a major role in government, and it therefore seems reasonable to recommend that:

> You task the GSA to compile such a comprehensive handbook of preferred practices and procedures for running a computer center securely.

It is not a big undertaking. It is not an endeavor for tens or dozens of people working for many years. One could survey the federal agencies and a selected set of large corporations, assemble the composite wisdom of what is being done and what is known, and get it written down. I would submit that it is a chore for a few people for a year or so.

Mr. Stephen Walker testified before you in September and suggested a Federal Center to undertake some of the tasks that I have suggested above be done by ICST and the GSA. Such a Federal Center would undoubtedly be a good idea and we clearly would well have it in the long run. CSC cannot do everything; moreover, some of its technical knowledge can never be shared because of vital defense secrets. But on the large, CSC represents an innovative opportunity for interaction between the federal government and the commercial sector. It can respond to technical issues and it can examine and certify commercial software products for trustworthiness; but CSC is not likely to concern itself with the less esoteric and more mundane issues that a Federal Center might accommodate. Until, and if, we get such an organization in place, however, there is no reason why the ICST and the GSA might not do what clearly can be done now.

I do not want to conclude this testimony without touching briefly on privacy. First, let me clarify a statement which I believe was made to you by Congressman Wirth. I disagree strongly with his observation that all the aspects of privacy have now been attended to. In fact, most of the recommendations that were made by the Privacy Protection Study Commission have not been implemented in law, and moreover there are new dimensions of privacy that the PPSC did not identify nor treat. To date, privacy has been interpreted in the context of record-keeping processes, but it is clear that the widespread application of computer and communication systems to provide a broad spectrum of services will eventuate in many new dimensions of privacy.

We are seeing the emergence of systems that contain vast amounts of information about people but not for record-keeping purposes. Let me illustrate in terms of electronic mail, which the U.S. Postal Service is promoting as E-COM. The purpose of such a service is to transport information from sender to addressee and to the extent that such information is personal in nature, the system will contain much information about people but not for record-keeping purposes. In addition to the message content, the system will contain information relating addressee to sender. In principle, such information could be used to establish relationships among groups of people, such as organized groups or circles of acquaintances. Obviously, such information could be of high interest to the law enforcement community, for the legal umbrella of protection over it is complex and probably incomplete.

Whatever one believes about the security of information in the hands of the USPS's E-COM, it is clear that private offerings of electronic mail, such as by MCI and GTE, are another question. In the case of the latter there is little, if any, legal protection for message information in the hands of private organizations.

I will develop the issue more fully with two examples relative to electronic mail. In a federal agency, the in-house investigative staff on at least three occasions obtained a complete printout of the electronic mail system that provides office-automation support. On at least one occasion, an outside law enforcement entity was also involved. In effect, several hundred workers who use electronic mail in the conduct of their business had all their computer records read, and in at least one instance, an individual was intimidated. The privacy of the workplace records of hundreds of people had been invaded; hundreds of people were caught up in an investigative sweep without recourse to protect themselves.

It all sounds very much like search-and-seizure without due process of law, or like a fishing expedition to see if something wrong had happened or if some crime had been committed. In this instance, the computer happened to be agency-owned; one wonders what the situation might have been if the mail service had been provided by a commercial vendor whose computer would be located on private premises?

I do not know the motivations of the investigative groups; I have only one side of the story. Perhaps they were tracking down hackers, or maybe it had to do with possible fraud or embezzlement. I have no wish to make this incident a cause celebre, but it is very useful to underscore the ease with which new privacy issues arise as computer and communications technology is exploited to provide a wide variety of new services to a wider and wider population of users.

It is an example of a new dimension of privacy -- "access without action"; computer matching of files exhibits the same dimension. Individuals who happen to keep records in a computer system or who are record subjects in a computer file have their privacy invaded whether or not an individual has done something wrong. Private information gets exposed to a third party and possibly to hostile eyes. In effect, all the hundreds of office workers or all the data subjects in a computer file have, a priori, been assumed to be guilty; the examination of mail or the matching of computer records is to demonstrate that they are not. Much information about people has been seen but no action taken. It sounds like a back-end-to process of justice.

There are some happy aspects of the office-automation seizure. In such a system, hundreds of people will keep hundreds of messages each; there will be tens-of-thousands of messages altogether. Only two aberrant ones were found: a baby sitter's phone number and a cooking recipe. The odds are that each item, admittedly personal, was transmitted more efficiently by electronic mail than by a phone call or a walk to another person's desk; the electronic mail system surely diverted much less people time from the job than any other means of interpersonal communication.

Certainly there are management problems in assuring that corporate or business resources are not used for personal reasons, but I admire the management discipline of an agency that operates such a tight facility -- two items out of many tens-of-thousands is really an infinitesimal ratio; and I acknowledge the integrity of the hundreds of people who are using it.

Let us examine the possibility that an agency of government were to use a commercial electronic mail service which is supplied by a computer host that is most likely not in the District.[3] There is no question but that electronic mail is an efficient mechanism to facilitate the conduct of business in any large organization; that is not the issue. What are the risks to such an arrangement? I can offer some considered observations -- which importantly would not be unique to any one private sector vendor.

- It is unlikely that the phone lines, whether dial-up or dedicated, between Washington and "the other state" would be protected by an encryption process. Electronic eavesdropping and wiretapping would therefore be possible threats.
- It is unlikely that the computer system would have special security safeguards because commercial equipment is often used for such services. One would assume that the vendor has provided appropriate physical, admininstative, and personnel safeguards.
- Since the electronic traffic would flow across state lines, it becomes a matter for federal law; but there is no law under which the information would be protected.
- In principle, the body of computer-contained electronic mail would be subject to the same seizure as the office workers experienced; the private vendor would have no legal standing to resist. While I would not suggest for a moment that some agency of government would set out to seize the electronic mail of another, a dissident group might and such mail could get caught up in an investigative sweep aimed at someone else.

[3]After the presentation of this testimony, the author's attention was called to a *New York Times* article ("White House Link: Computer in Ohio"; David Burnham, July 13, 1983, Late City Final Edition, page 18, section A, column 4) which describes the Executive Data Network which provides the Executive Branch of government with electronic mail services from a system in Columbus, Ohio. The article also reported by name the officials who were to use it.

Why all my emphasis on both security and privacy of electronic mail? You must not think of electronic mail as solely the electronic analog of the envelope. Perhaps one fourth of my business interactions and transactions occur electronically; at the moment there are about 600 messages in my mailbox and it can get as high as a thousand. Why? It represents the written record of my conduct of business with a variety of individuals and organizations; it is much more efficient than writing letters, making phones calls, and then writing memoranda-of-record. Moreover, I can organize the messages by folders and subfolders so that the system becomes a comprehensive automated filing and information retrieval system. Anyone having access to such a body of information might as well have the key to the office and to its file cabinets.

Such comprehensive business records service is what electronic mail is really all about, and it is the service that will be offered by the private sector. Can you imagine the situation when all that information -- both private and corporate -- gets into electronic mail systems? Can you imagine what a lucrative target it will become for all sorts of reasons? The computer matching we have seen so far will be nothing compared to what might arise when someone thinks about comparing files from electronic mail systems.

Here are some of the issues for information in such systems:

- It is not clear who owns it. Does the owner of the computer system per se own it? Does he have the right to witch-hunt through the information in his system as he sees fit? Or is asked to by a third party?
- It is not clear if, or by what law, it is protected. What will be the situation for intrastate offerings of service vs. interstate offerings? And in the long run, for international offerings?
- It is not clear what the search-and-seizure situation is; can the private vendor be given legal standing to resist? What should be his obligations to the users of his system in case of attempted seizure?

- It is not even clear what the liability of the purveyor of the service might be, should something happen to one's electronic mail records. What is his responsibility or obligation if his system accidentally spills information to the wrong party? What is his responsibility if his maintenance people accidentally see such mail information and use it for private gain, for personal embarrassment, for political advantage, or for a breach of national welfare and security?
- What are the vendor's obligations to provide comprehensive security safeguards for his system? Should they be mandated by law? Should it be caveat emptor? For private sector and government use alike? Should the government be concerned that so much corporate information might be subject to penetration by unfriendly agents?
- How should electronic mail be treated relative to telephone conversations? Over the years, certain privacy protections have arisen for telephone billing records; formal legal processes are necessary to wiretap or to obtain records. Should similar protections exist for electronic mail? Within government, as well as in private sector, as well as in regulated public utility?

Many of these same concerns will also be pertinent to other systems. For example, there is voice mail which is the spoken analog of electronic mail -- a service which is actively being promoted by private vendors and by various telephone companies. Voice mail has all the vulnerabilities that electronic mail has when offered by public vendors. Moreover, an intruder can always claim that a particular individual's voice can be recognized although his typed signature can be forged by someone else at the keyboard. Encryption techniques can be used to protect electronic mail but present systems do not offer sender-to-reader encryption options. It is much more difficult technically to provide speaker-to-listener protection for voice mail.

There is, in addition, the body of information which is collected about people by point-of-sale systems, by debit card systems on the merchant's premises, by automated checkout stands in grocery stores, and a whole host of others. In each case the system exists for some purpose other than the traditional record-keeping one; each happens to contain information about people as a collateral consequence of its primary intent. But the whole subject of privacy ahead, of what the future holds for privacy, of what its new dimensions are, is for another day; I have left you just a little teaser of what it will be all about. Clearly, electronic mail is upon us now.

Let me speak to the issue of a National Commission. Congressman Wirth and Mr. Parker suggested to you on September 26 that a national commission to investigate computer crime would be appropriate. A year or so ago I suggested at a National Computer Conference that a National Commission would be an appropriate forum in which to examine possible vulnerabilities of our highly computerized society. The fact is that there is a whole set of interrelated issues that could well be collectivly examined by a congressionally chartered commission. The common element to all of them is information handling as performed by computer and communication systems. Included would be such things as computer-related crime, new dimensions of privacy, national vulnerability as a result of computerization, representation of information, social consequences of intensive computerization, personal identification in a highly automated society, dislocations of power as a result of concentrations of information, and others.

My personal experience with the Privacy Protection Study Commission persuaded me that a congressionally chartered commission is an appropriate mechanism to address broad national issues that transcend the jurisdictional boundaries of federal agencies and also transcend public and private sector interests. Such a commission can provide an enormous bargain for the country in terms of work accomplished. For example, the PPSC delivered about 60 man-years of research on the subject of record-keeping practices in the private sector for about $2.5 million. That equates to about $40,000 per person-year of effort which is about one third of what it would cost if done by a contractor. In my

view there is a right and a wrong way to structure a commission, but that is a subject for another time if the Congress should be persuaded to move that way.

Congressman Glickman, I have given you a once-over-lightly on some aspects of a very intricate and complex issue. I would be glad to deal in more depth with such aspects as you may wish, either in writing or personal discussion with your staff. There must be a national concern for providing adequate security protections in our public and private information systems and for attending the new privacy issues that arise. We know a lot about doing it, but it needs to be organized into a concerted effort. If the Congress has the will to pursue this issue and to pay sufficient attention to it, my feeling is that the time is right for action.

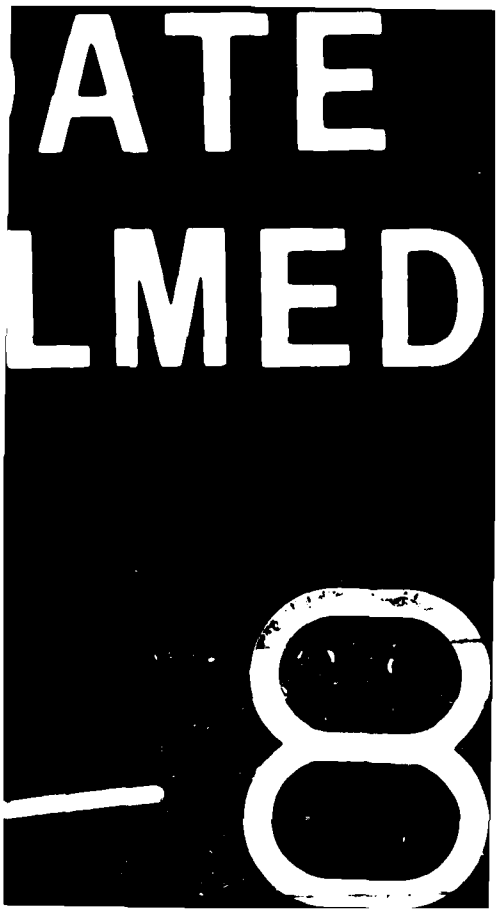
To begin with, let's get the GSA going; let's put ICST to work; let's address electronic mail as the most pressing of the new dimensions of privacy. Let's think about making 1984 "the right year" to launch a Commission to comprehensively examine the many issues of which we have talked.

[At the conclusion of the testimony and questions, the chairman, Congressman Glickman, read excerpts from a *New York Times* article ("Computer Intrusion Reported in 18 Companies and U.S. Agencies"; Joseph B. Treaster, Sunday, October 23, 1983, page 21). It described the penetration of the Telemail service offered by GTE, and the apparent access to the electronic mail of major U.S. companies such as Raytheon, Coca Cola U.S.A., the 3M Company, and of several federal agencies such as NASA and the Department of Agriculture.]

Note added in proof:

Subsequent to the completion of this document, a *New York Times* article discussed the incident referenced anonymously on page 11 above ("Can Privacy and Computer Coexist?"; David Burnham, Saturday, November 5, 1983, page 11). It identified the "federal agency" as the Army's DARCOM, the "in-house investigative staff" as the Army's Criminal Investigation Division, and the "outside law enforcement entity" as the

FBI. It also mentions that the incident was originally described in an ARPANET message and includes quotes from it. In addition, it paraphrases three responses from various individuals.


ATE
LMED
8